

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-14796

(P2001-14796A)

(43) 公開日 平成13年 1月19日 (2001.1.19)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 C 0 5 3
H 0 4 N 5/91		H 0 4 N 5/91	P 5 C 0 6 3
7/08		7/08	Z 5 D 0 4 4
7/081			

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号	特願平11-233446	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目 6 番地
(22) 出願日	平成11年 8 月20日 (1999. 8. 20)	(72) 発明者	▲高▼橋 将 神奈川県横浜市戸塚区吉田町292番地 株 式会社日立製作所デジタルメディア開発本 部内
(31) 優先権主張番号	特願平11-121253	(72) 発明者	竹内 敏文 神奈川県横浜市戸塚区吉田町292番地 株 式会社日立製作所デジタルメディア開発本 部内
(32) 優先日	平成11年 4 月28日 (1999. 4. 28)	(74) 代理人	100075096 弁理士 作田 康夫
(33) 優先権主張国	日本 (J P)		

最終頁に続く

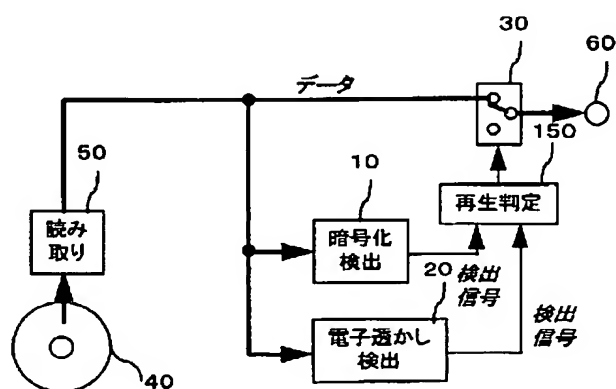
(54) 【発明の名称】 再生装置および復号装置

(57) 【要約】

【課題】電子透かしの誤検出によって所定の暗号方式で暗号化された正規な蓄積媒体の再生も不可となってしまう。

【解決手段】暗号化されていない場合にのみ電子透かし検出およびこれによる再生制限を行う。暗号化検出回路 (10) により所定の暗号方式で暗号化されていないことが検出され、電子透かし検出回路 (20) により電子透かし情報が検出された場合に、再生制限回路 (30) による再生停止を行う。暗号化検出回路 (10) により所定の暗号方式で暗号化されていることが検出された場合は、再生制限回路 (30) は再生を停止しない。

図1



【特許請求の範囲】

【請求項 1】蓄積媒体に記録された映像または音声情報を再生する再生装置において、

蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されているかどうかを検出する暗号化検出手段と、

蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、

蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合には電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に映像または音声情報の再生を停止する再生制限手段を有することを特徴とする再生装置。

【請求項 2】請求項 1 に記載の再生装置において、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に蓄積媒体に記録された映像または音声情報が電子透かし検出手段において電子透かし情報を検出できるような正規な映像または音声情報であるかどうかを解析する情報解析手段を有し、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に、情報解析手段によって電子透かし情報を検出できるような正規な映像または音声情報ではないと判定された時にも、前記再生制限手段は映像または音声情報の再生を停止することを特徴とする再生装置。

【請求項 3】符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力する復号装置において、

暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元する暗号解読手段と、暗号解読手段を用いなくて入力された符号化された映像または音声情報を直接復号する場合に復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、

暗号解読手段を用いなくて入力された符号化された映像または音声情報を直接復号する場合には、電子透かし検出手段によって何らかの複製管理情報が検出された時に映像または音声情報の出力を停止する出力制限手段を有することを特徴とする復号装置。

【請求項 4】請求項 1 に記載の再生装置において、複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォーマット判別手段を備え、

暗号化検出手段は前記複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットそれぞれに定められた暗号方式で暗号化されているかどうかを検出する手段であり、

蓄積媒体に記録された映像または音声情報が、媒体およびフォーマット判別手段で判別された蓄積媒体の種類および蓄積媒体上の記録フォーマットで定められた暗号方式で暗号化されていない場合には、電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に、再生制限手段は映像または音声情報の再生を停止することを特徴とする再生装置。

【請求項 5】符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力する復号装置において、

暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元する暗号解読手段と、入力符号化データの供給装置との間の認証と暗号解読に必要なキー交換を行う AKE 手段と、

AKE 手段で認証およびキー交換が成立しない状態で復号を開始した時に、復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、

AKE 手段で認証およびキー交換が成立しない状態で復号を開始した時には、電子透かし検出手段によって何らかの複製管理情報が検出された時に、映像または音声情報の出力を停止する出力制限手段を有することを特徴とする復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は著作権保護に関し、正規に販売あるいは配布された蓄積媒体および正規に記録された蓄積媒体は再生可能とし、違法に複製された媒体は再生不可とする再生装置、および、正規に販売あるいは配布された蓄積媒体および正規に記録された蓄積媒体から再生した符号は復号可能とし、違法に複製された媒体から再生した符号は復号不可とする復号装置に関する。

【0002】

【従来の技術】ビデオディスク、デジタル VTR、ディジタル放送の受信装置などにより得られる高画質のビデオ信号に対する著作権保護を確実に行うようにしたビデオ信号処理装置や、ビデオ信号処理方法、記録媒体に関する技術については、例えば、特開平 10-178656 号公報に記載されている。また、コピー防止のための認証と KEY 交換については、例えば、日経エレクトロニクス (NIKKEI ELECTRONICS 1998.3.23(N0712)P47~P53) に記載されている。

【0003】

【発明が解決しようとする課題】前記公報には世代管理情報を用いた複製防止技術が示されている。しかし、違法に作成された蓄積媒体の再生を不可とする技術にまでは言及されていない。

【0004】複製防止を確実に行うためには、暗号化の技術が有効である。蓄積媒体に記録する映像または音声

情報を暗号化し、契約を結んだ者にだけ暗号を解く鍵を供給することにより、違法に作成された蓄積媒体の再生を不可とすることができる。

【0005】しかし、暗号を解いて再生した映像または音声情報は自由に他の蓄積媒体に記録できてしまい、複製防止にならない。このような複製を防止するためには、世代管理情報を映像または音声情報上に、視聴しても検知できない形で重畳する、いわゆる電子透かし技術が有効である。すなわち、記録する映像または音声情報の電子透かしを検出して記録の制限を行ったり、再生した映像または音声情報の電子透かしを検出して再生の制限を行ったりして違法な複製および違法に複製された映像または音声情報の視聴の防止に役立てることができる。

【0006】暗号化技術と電子透かし技術を併用することにより、複製防止をより確実に行うことができる。すなわち、著作権を保護したい映像または音声情報には必ず電子透かしを付け、かつ蓄積媒体上では必ず暗号化するようにすればよい。しかし、従来の技術は、暗号化技術と電子透かし技術を併用した場合にどのようにして違法に作成された蓄積媒体の再生を不可とするかについて考慮されていなかった。特に、電子透かしの誤検出によって正規に販売あるいは配布された蓄積媒体および正規に記録された蓄積媒体の再生も不可になってしまう問題について考慮されていなかった。

【0007】本発明の目的は、暗号化と電子透かしを併用した場合に、違法に作成された蓄積媒体については視聴できないようにし、正規に作成され販売あるいは配布された蓄積媒体、あるいは正規の方法に従い記録した蓄積媒体については再生し視聴することのできる様にした技術、特に、電子透かしの誤検出によって正規に販売あるいは配布された蓄積媒体および正規に記録された蓄積媒体の再生および視聴も不可になってしまう問題を回避する技術を示し、これらの技術を用いた再生装置および復号装置を提供することである。

【0008】

【課題を解決するための手段】本発明に関する再生装置は、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されているかどうかを検出する暗号化検出手段と、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合には電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に映像または音声情報の再生を停止する再生制限手段を有することを特徴とする。

【0009】また、本発明に関する再生装置は、蓄積媒体に記録された映像または音声情報が所定の暗号方式で

暗号化されていない場合に蓄積媒体に記録された映像または音声情報が電子透かし検出手段において電子透かし情報を検出できるような正規な映像または音声情報であるかどうかを解析する情報解析手段と、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合には情報解析手段によって電子透かし情報を検出できるような正規な映像または音声情報ではないと判定された時にも映像または音声情報の再生を停止する再生制限手段を有することを特徴とする。

10 【0010】さらにまた、本発明に関する復号装置は、暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元する暗号解読手段と、暗号解読手段を用いず入力符号化データを直接復号する場合に復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、暗号解読手段を用いず入力符号化データを直接復号する場合には電子透かし検出手段によって何らかの複製管理情報が検出された時に映像または音声情報の出力を停止する出力制限手段を有することを特徴とする。

20 【0011】さらに、本発明に関する再生装置は、複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォーマット判別手段と、前記複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットそれぞれに定められた暗号方式で暗号化されているかどうかを検出する暗号化検出手段と、蓄積媒体に記録された映像または音声情報が、媒体およびフォーマット判別手段で判別された蓄積媒体の種類および蓄積媒体上の記録フォーマットで定められた暗号方式で暗号化されていない場合には、電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に、映像または音声情報の再生を停止する再生制限手段を有することを特徴とする。

30 【0012】また、本発明に関する復号装置は、暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元する暗号解読手段と、入力符号化データの供給装置との間の認証と暗号解読に必要なキー交換を行うAKE (Authentication and Key Exchange) 手段と、AKE手段で認証およびキー交換が成立しない状態で復号を開始した時に、復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、AKE手段で認証およびキー交換が成立しない状態で復号を開始した時には、電子透かし検出手段によって何らかの複製管理情報が検出された時に、映像または音声情報の出力を停止する出力制限手段を有することを特徴とする。

【0013】

50 【発明の実施の形態】以下、本発明の実施の形態を図面を用いて詳細に説明する。

【0014】図1は、本発明に係わる再生装置の実施例の信号の流れを示したブロック図である。図1において、10は暗号化検出回路、20は電子透かし検出回路、30は再生制限回路、40は蓄積媒体、50は読み取り回路、60は再生データ出力端子、150は再生判定回路である。

【0015】本実施例は、DVD-ROMやDVD-RAMなどの蓄積媒体を再生するいわゆるドライブである。読み取り回路50は蓄積媒体40からデータを読み取り、読み取った符号化データを暗号化検出回路10、電子透かし検出回路20及び再生制限回路30へ供給する。

【0016】例えば、DVD-ROMでは、記録する映像情報の著作権を保護するため、MPEG2方式で圧縮符号化された動画データデータを暗号化して記録する方式が用意されており、DVD-RAMでも同様の方式が検討されている。また、暗号を解いてしまった映像情報に対しても複製の制限を行うようにするために、複製管理情報を映像情報上に直接、視聴しても検知できない形で重畳する電子透かし方式が検討されている。本実施例は、これらの暗号化されたり、電子透かしが入れられたりしたDVD-ROMやDVD-RAMを再生することができる。

【0017】暗号方式検出回路10は、蓄積媒体40上に記録された、所定の暗号方式で暗号化されたディスクであることを示す情報を検出する。

【0018】電子透かし検出回路20は、蓄積媒体40上に記録された映像情報に重畳された電子透かしを検出する。

【0019】再生判定回路150は、条件に応じて、再生データ出力端子60から動画データを出力するかどうかを判定し、再生制限回路30は判定結果に応じて、出力する場合には再生データ出力端子60へ動画データを供給し、出力しない場合には再生データ出力端子60へ信号を供給しない。図2は、再生条件を示した図である。暗号化されているディスクの場合は、著作権保護された正規なディスクなので再生する。暗号化されていないディスクの場合で、電子透かし検出回路20により電子透かしが検出された場合は、違法に複製されたディスクと見なし、再生を停止する。暗号化されていないディスクの場合で、電子透かし検出回路20により電子透かしが検出されなかった場合は、著作権保護されていないディスクなのでそのまま再生する。これにより、違法に複製されたディスクの視聴を止めることができ、暗号化された正規なディスクを再生した時に電子透かしが誤検出されても誤って再生停止してしまうことがない。

【0020】図3は、本発明に係わる再生装置の実施例の信号の流れを示したブロック図である。図3において、10は暗号化検出回路、20は電子透かし検出回路、30は再生制限回路、40は蓄積媒体、50は読み

取り回路、60は再生データ出力端子、70は情報解析回路、150は再生判定回路である。

【0021】本実施例も、DVD-ROMやDVD-RAMなどの蓄積媒体を再生するいわゆるドライブである。読み取り回路50は蓄積媒体40からデータを読み取り、読み取った符号化データを暗号化検出回路10、電子透かし検出回路20、再生制限回路30および情報解析回路70へ供給する。

【0022】暗号方式検出回路10は、蓄積媒体40上に記録された、所定の暗号方式で暗号化されたディスクであることを示す情報を検出する。

【0023】電子透かし検出回路20は、蓄積媒体40上に記録された映像情報に重畳された電子透かしを検出する。

【0024】情報解析回路70は、電子透かし検出回路20への入力データが電子透かしの検出回路が可能な正規な入力データであるかどうかを解析する。具体的には、本実施例では、MPEG2方式に合致した正規なデータであるかどうかを調べる。

【0025】再生判定回路150は、条件に応じて、再生データ出力端子60から動画データを出力するかどうかを判定し、再生制限回路30は判定結果に応じて、出力する場合には再生データ出力端子60へ動画データを供給し、出力しない場合には再生データ出力端子60へ信号を供給しない。図4は、再生条件を示した図である。暗号化されているディスクの場合は、著作権保護された正規なディスクなので再生する。暗号化されていないディスクの場合で、電子透かし検出回路20により電子透かしが検出された場合は、違法に複製されたディスクと見なし、再生を停止する。暗号化されていないディスクの場合で、電子透かし検出回路20により電子透かしが検出されなかった場合は、かつ、電子透かしの検出が可能な正規な入力データである場合は、著作権保護されていないディスクなのでそのまま再生する。暗号化されていないディスクの場合で、電子透かし検出回路20により電子透かしが検出されなかった場合は、かつ、電子透かしの検出が不可能でない不正な入力データである場合は、電子透かしの検出が不能になるように違法に暗号化されたディスクと見なし、再生を停止する。これにより、電子透かしの検出が不能になるように違法に暗号化されたディスクの視聴も止めることができる。

【0026】図5は、本発明に係わる復号装置の実施例の信号の流れを示したブロック図である。図5において、20は電子透かし検出回路、80は暗号解読回路、90は出力制限回路、100は符号化データ入力端子、110は暗号解読有無指定入力端子、120は選択回路、130は復号回路、140は復号データ出力端子、160は出力判定回路である。

【0027】本実施例は、MPEG2方式で圧縮符号化された動画データを復号するいわゆるデコーダボード

である。符号化データ入力端子 100 には DVD-ROM や DVD-RAM などの蓄積媒体から再生された符号化データが入力される。

【0028】本実施例は、暗号化された DVD-ROM や DVD-RAM から再生される符号化データを復号することができる。暗号解読回路 80 がこの暗号を解く回路である。

【0029】暗号解読有無指定入力端子 110 には、暗号化されたディスクを再生する場合には暗号解読することを指示する信号が入力され、その他の場合には暗号解読しないことを指示する信号が入力される。選択回路 120 は暗号解読する場合には暗号解読回路 80 で暗号解読された符号化データを選択し、暗号解読しない場合には符号化データ入力端子 100 に入力された符号化データを選択し、復号回路 130 へ供給する。復号回路 130 は MPEG2 方式に基づく復号処理を行い、動画像データを復号する。復号された動画像データは復号データ出力端子 140 から出力される。

【0030】出力判定回路 160 は、条件に応じて、復号データ出力端子 140 から動画像データを出力するかどうかを判定し、出力制限回路 90 は判定結果に応じて、出力する場合には復号データ出力端子 140 へ動画像データを供給し、出力しない場合には復号データ出力端子 140 へ信号を供給しない。図 6 は、出力条件を示した図である。暗号解読する場合は、著作権保護された正規な符号なので出力する。暗号解読しない場合で、電子透かし検出回路 20 により電子透かしが検出された場合は、違法に複製されたディスクの再生データと見なし、出力を停止する。暗号解読しない場合で、電子透かし検出回路 20 により電子透かしが検出されなかった場合は、著作権保護されていない符号なのでそのまま再生する。これにより、違法に複製されたディスクからの再生データの視聴を止めることができ、暗号化された正規なディスクからの再生データを復号した時に電子透かしが誤検出されても誤って出力停止してしまうことがない。

【0031】以上述べた実施例の説明は全て映像情報の場合を説明したが、音声情報の場合も、映像の符号化、復号化が音声の符号化、復号化になり、映像の電子透かしが音声の電子透かしになるだけで、実施例の構成は同様で、同様の効果が得られる。

【0032】図 7 は、複数の種類の蓄積媒体に対応した再生装置の実施例の信号の流れを示したブロック図である。図 7 において、10 は暗号化検出回路、20 は電子透かし検出回路、30 は再生制限回路、40 は蓄積媒体、50 は読み取り回路、60 は再生データ出力端子、150 は再生判定回路、170 は媒体及びフォーマット判別回路である。

【0033】本実施例は、DVD-ROM と DVD-RAM の複数種類の蓄積媒体を再生するドライブである。

読み取り回路 50 は蓄積媒体 40 からデータを読み取り、読み取った符号化データを暗号化検出回路 10、電子透かし検出回路 20、媒体及びフォーマット判別回路 170 および再生制限回路 30 へ供給する。

【0034】DVD-ROM の画像情報用（いわゆる DVD-Video フォーマット）に用意されている暗号方式は、CSS (Content Scrambling System) 方式と呼ばれている。DVD-RAM でも同様の方式が検討されているが、CSS 方式とは異なる暗号方式である。また、DVD-RAM の中でも、画像情報を MPEG2 方式で圧縮符号化しながら記録するためのリアルタイム記録フォーマットと、MPEG2 方式で圧縮符号化済みのビットストリームをそのまま記録するためのストリーム記録フォーマットがある。ストリーム記録の場合は、圧縮符号化済みのビットストリームが暗号化された状態で送られてくる。リアルタイム記録フォーマットの暗号方式とストリーム記録フォーマットの暗号方式も、異なる暗号方式になると予想される。本実施例は、これら全てのディスクおよび暗号方式に対応した再生を行うことができる。

【0035】媒体及びフォーマット判別回路 170 は、蓄積媒体 40 の種類と記録フォーマットを判別する。

【0036】暗号方式検出回路 10 は、蓄積媒体 40 の種類と記録フォーマットに応じて定められた所定の暗号方式で暗号化されていることを示す情報を検出する。

【0037】電子透かし検出回路 20 は、蓄積媒体 40 上に記録された映像情報に重畳された電子透かしを検出する。

【0038】再生判定回路 150 は、条件に応じて、再生データ出力端子 60 から動画像データを出力するかどうかを判定し、再生制限回路 30 は判定結果に応じて、出力する場合には再生データ出力端子 60 へ動画像データを供給し、出力しない場合には再生データ出力端子 60 へ信号を供給しない。図 8 は、再生条件を示した図である。DVD-ROM の Video フォーマットで暗号方式が CSS 方式の場合は、著作権保護された正規なディスクなので再生する。DVD-RAM のリアルタイム記録フォーマットで暗号方式がリアルタイム記録フォーマット用暗号方式の場合は、著作権保護された正規なディスクなので再生する。DVD-RAM のストリーム記録フォーマットで暗号方式がストリーム記録フォーマット用暗号方式の場合は、著作権保護された正規なディスクなので再生する。各フォーマットにおいて、暗号化されていないディスクの場合で、電子透かし検出回路 20 により電子透かしが検出された場合は、違法に複製されたディスクと見なし、再生を停止する。暗号化されていないディスクの場合で、電子透かし検出回路 20 により電子透かしが検出されなかった場合は、著作権保護されていないディスクなのでそのまま再生する。

【0039】本実施例によれば、異なる暗号方式が定め

られた複数種類の記録フォーマットのディスクを再生する場合にも、違法に複製されたディスクの視聴を止めることができ、暗号化された正規なディスクを再生した時に電子透かしが誤検出されても誤って再生停止してしまいうことがない。

【0040】図9は、AKE付き復号装置の実施例の信号の流れを示したブロック図である。図9において、20は電子透かし検出回路、80は暗号解読回路、90は出力制限回路、100は符号化データ入力端子、120は選択回路、130は復号回路、140は復号データ出力端子、160は出力判定回路、180はAKE回路である。

【0041】本実施例は、MPEG2方式で圧縮符号化された動画像データを復号するいわゆるデコーダボードである。符号化データ入力端子100にはDVD-ROMやDVD-RAMなどの蓄積媒体から再生された符号化データが入力される。

【0042】本実施例はAKE回路180を内蔵し、DVD-ROMドライブやDVD-RAMドライブなどの外部装置から暗号化された符号化データを受け取って復号する場合には、AKE回路180により外部装置との間で認証とキー交換（いわゆるAKE）を行ってキーを取得し、このキーを用いて暗号解読を行う。暗号解読回路80がこの暗号を解く回路である。

【0043】選択回路120はAKEが成立して暗号解読する場合には暗号解読回路80で暗号解読された符号化データを選択し、AKEが成立せず暗号解読しない場合には符号化データ入力端子100に入力された符号化データを選択し、復号回路130へ供給する。復号回路130はMPEG2方式に基づく復号処理を行い、動画像データを復号する。正規なMPEG2データが入力され、復号が開始された場合には、電子透かし検出回路20および出力判定回路160へ検出信号を送る。復号された動画像データは復号データ出力端子140から出力される。

【0044】電子透かし検出回路20は、AKEが成立せず復号が開始された場合に、復号された動画像データの電子透かしを検出する。

【0045】出力判定回路160は、条件に応じて、復号データ出力端子140から動画像データを出力するかどうかを判定し、出力制限回路90は判定結果に応じて、出力する場合には復号データ出力端子140へ動画像データを供給し、出力しない場合には復号データ出力端子140へ信号を供給しない。図10は、出力条件を示した図である。AKEが成立して暗号解読する場合で、復号が動作した場合は、著作権保護された正規な符号なので出力する。AKEが成立せず暗号解読しない場合で、復号が動作した場合は、電子透かし検出回路20により電子透かしが検出された場合、違法に複製されたディスクの再生データと見なし、出力を停止する。AKE

Eが成立せず暗号解読しない場合で、復号が動作した場合で、電子透かし検出回路20により電子透かしが検出されなかった場合は、著作権保護されていない符号なのでそのまま出力する。復号が動作しなかった場合は、出力を停止する。出力しても良いが、復号が動作していないので、この時は意味のある動画像データは出力されない。

【0046】これにより、AKEの動作しない違法に複製されたディスクからの再生データの視聴を止めることができ、AKEが動作する暗号化された正規なディスクからの再生データを復号した時に電子透かしが誤検出されても誤って出力停止してしまいうことがない。

【0047】

【発明の効果】本発明によれば、蓄積媒体に記録された映像または音声情報を再生する再生装置において、所定の暗号方式で暗号化されていない蓄積媒体については電子透かしがあれば再生を止められるので違法に複製された蓄積媒体の視聴を止めることができ、所定の暗号方式で暗号化されている正規な蓄積媒体については電子透かし情報が誤検出されたとしても確実に再生が行われる。

【0048】また、本発明によれば、電子透かし情報が検出されないように違法な暗号方式で暗号化されている場合にも再生を止めることができる。

【0049】さらにはまた、本発明によれば、符号化された映像または音声情報を復号する復号装置において、所定の暗号方式で暗号化されていない符号については電子透かしがあれば復号を止められるので違法に複製された蓄積媒体からの符号を復号しての視聴を止めることができ、所定の暗号方式で暗号化されている正規な符号については電子透かし情報が誤検出されたとしても確実に復号が行われる。

【0050】さらに、本発明によれば、異なる暗号方式が定められた複数種類の記録フォーマットの蓄積媒体を再生する場合にも、違法に複製された蓄積媒体の視聴を止めることができ、所定の暗号方式で暗号化されている正規な蓄積媒体については電子透かし情報が誤検出されたとしても確実に再生が行われる。

【0051】また、本発明によれば、AKEの動作しない違法に複製された蓄積媒体からの符号を復号しての視聴を止めることができ、AKEが動作する正規な符号については電子透かし情報が誤検出されたとしても確実に復号が行われる。

【図面の簡単な説明】

【図1】本発明に係わる再生装置の実施例のブロック図。

【図2】本発明に係わる再生装置の実施例の再生条件を示す図。

【図3】本発明に係わる再生装置の実施例のブロック図。

【図4】本発明に係わる再生装置の実施例の再生条件を

示す図。

【図5】本発明に係わる復号装置の実施例のブロック図。

【図6】本発明に係わる復号装置の実施例の出力条件を示す図。

【図7】本発明に係わる再生装置の実施例のブロック図。

【図8】本発明に係わる再生装置の実施例の再生条件を示す図。

【図9】本発明に係わる復号装置の実施例のブロック

図。 【図10】本発明に係わる復号装置の実施例の出力条件＊

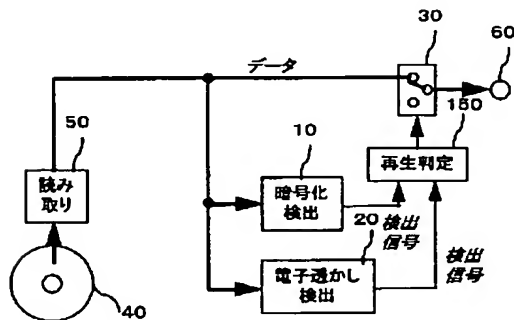
＊を示す図。

【符号の説明】

10…暗号化検出回路、20…電子透かし検出回路、30…再生制限回路、40…蓄積媒体、50…読み取り回路、60…再生データ出力端子、70…情報解析回路、80…暗号解読回路、90…出力制限回路、100…符号化データ入力端子、110…暗号解読有無指定入力端子、120…選択回路、130…復号回路、140…復号データ出力端子、150…再生判定回路、160…出力判定回路、170…媒体及びフォーマット判別回路、180…AKE回路。

【図1】

図1



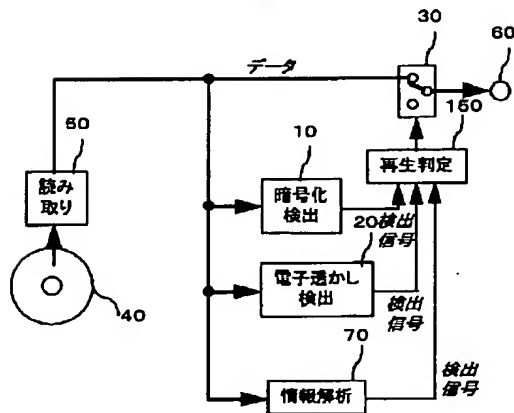
【図2】

図2

暗号方式検出	電子透かし検出	再生
所定の方法である	—	する
所定の方法以外 または 暗号無し	された	しない
	されなかった	する

【図3】

図3



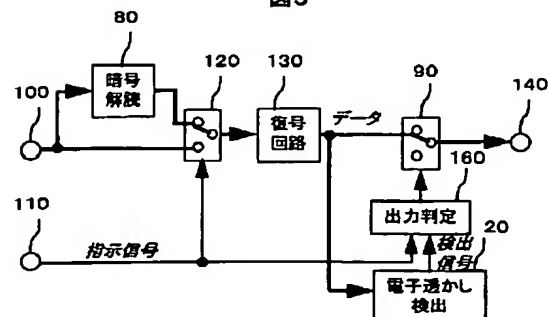
【図4】

図4

暗号方式検出	電子透かし検出	情報解析結果	再生
所定の方法である	—	—	する
所定の方法以外 または 暗号無し	された	—	しない
	されなかった	検出可能 検出不可能	する しない

【図5】

図5



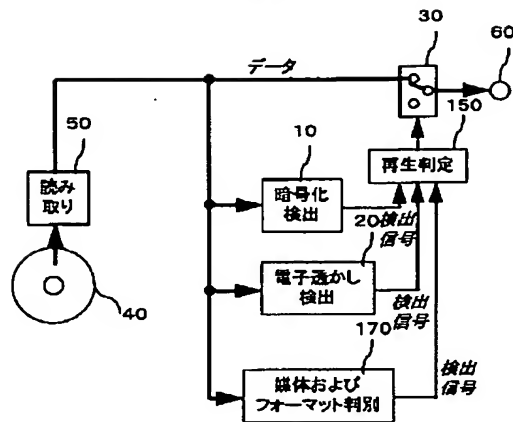
【図6】

図6

暗号解読	電子透かし検出	出力
する	—	する
しない	された	しない
	されなかった	する

【図7】

図7



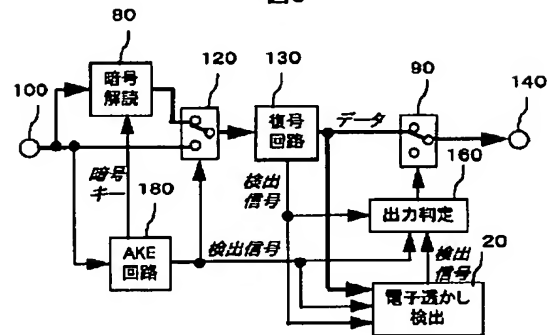
【図8】

図8

記録媒体	フォーマット	暗号方式検出	電子透かし検出	再生
DVD-ROM	ビデオ	CSS方式	—	する
		なし	された	しない
			されなかった	する
DVD-RAM	リアルタイム記録	リアルタイム記録用暗号方式	—	する
		なし	された	しない
			されなかった	する
	ストリーム記録	ストリーム記録用暗号方式	—	する
		なし	された	しない
			されなかった	する

【図9】

図9



【図10】

図10

AKE	暗号解読	復号	電子透かし検出	出力
動作した	する	動作した	—	する
動作しない	しない		された	しない
			されなかった	する
動作した	する	動作しない	—	しない
動作しない	しない			

フロントページの続き

(72)発明者 川前 治

神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

F ターム(参考) 5C053 FA13 FA20 FA21 FA23 GA11
GB06 GB11 GB38 HA29 JA03
KA21 KA24 LA06
5C063 AA01 AB03 AB05 AC01 AC05
CA11 CA36 DA07
5D044 AB05 AB07 DE49 DE50 EF05
FG18 GK11 GK17 HL08

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第6部門第4区分
 【発行日】平成16年11月25日(2004.11.25)

【公開番号】特開2001-14796(P2001-14796A)

【公開日】平成13年1月19日(2001.1.19)

【出願番号】特願平11-233446

【国際特許分類第7版】

G 1 1 B 20/10

H 0 4 N 5/91

H 0 4 N 7/08

H 0 4 N 7/081

【F I】

G 1 1 B 20/10 H

H 0 4 N 5/91 P

H 0 4 N 7/08 Z

【手続補正書】

【提出日】平成15年12月10日(2003.12.10)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

蓄積媒体に記録された映像または音声情報を再生する再生装置において、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されているかどうかを検出する暗号化方式検出手段と、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合には電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に映像または音声情報の再生を複製管理情報に従って制御する再生制限手段を有することを特徴とする再生装置。

【請求項2】

請求項1に記載の再生装置において、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に、蓄積媒体に記録された映像または音声情報が電子透かし検出手段において電子透かし情報を検出できるような正規な映像または音声情報であるかどうかを解析する情報解析手段を有し、蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に、情報解析手段によって電子透かし情報を検出できるような正規な映像または音声情報ではないと判定された時に、前記再生制限手段は映像または音声情報の再生を停止することを特徴とする再生装置。

【請求項3】

符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力する復号装置において、入力符号化データが暗号化されているかいないかに従って暗号解読の要・不要を示す暗号解読指定入力手段と、暗号化された入力符号化データを解読してもとの符号化された映像

または音声情報を復元する暗号解読手段と、暗号解読手段からの出力と暗号解読手段を用いない出力を切り替える選択手段と、切り替え手段から出力された符号化された映像または音声情報を復号する復号手段と、復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段とを備え、

暗号解読手段を用いないで入力された符号化された映像または音声情報を直接復号する場合には、電子透かし検出手段によって何らかの複製管理情報が検出された時に映像または音声情報の出力を複製管理情報に従って制御する出力制限手段を有することを特徴とする復号装置。

【請求項 4】

請求項 1 に記載の再生装置において、

複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォーマット判別手段を備え、

前記暗号化方式検出手段は前記複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットそれぞれに対応した暗号方式で暗号化されているかどうかを検出する手段であり、

蓄積媒体に記録された映像または音声情報が、媒体およびフォーマット判別手段で判別された蓄積媒体の種類および蓄積媒体上の記録フォーマットに対応した暗号方式で暗号化されていない場合において、前記電子透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に、再生制限手段は映像または音声情報の再生を複製管理情報に従って制御することを特徴とする再生装置。

【請求項 5】

符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力する復号装置において、

暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元する暗号解読手段と、

入力符号化データの供給装置との間の認証と暗号解読に必要なキー交換を行う A K E 手段と、

暗号解読手段からの出力と暗号解読手段を用いない出力を切り替える選択手段と、

前記選択手段から出力された符号化された映像または音声情報を復号する復号手段と、

復号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段とを備え、

A K E 手段で認証およびキー交換が成立しない状態で復号を開始した時には、電子透かし検出手段を動作させ、前記電子透かし検出手段によって何らかの複製管理情報が検出された時に、映像または音声情報の出力を複製管理情報に従って制御する出力制限手段を有することを特徴とする復号装置。

【請求項 6】

蓄積媒体に記録された映像または音声情報を再生する再生方法において、

蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されているかどうかを検出する暗号化方式検出ステップと、

前記暗号化方式検出ステップにより蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に、映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出ステップと、

前記電子透かし検出ステップの検出結果によって何らかの複製管理情報が検出された時に、映像または音声情報の再生を複製管理情報に従って制御する再生制限ステップを有することを特徴とする再生方法。

【請求項 7】

請求項 6 に記載の再生方法において、

複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォーマット判別ステップを備え、

前記暗号化方式検出ステップは前記複数の蓄積媒体の種類および蓄積媒体上の記録フォー

マットそれぞれに対応した暗号方式で暗号化されているかどうかを検出するステップであり、
前記媒体およびフォーマット判別ステップで判別された蓄積媒体の種類および蓄積媒体上の記録フォーマットに対応した暗号方式で暗号化されていない場合には、映像または音声情報の再生を停止することを特徴とする再生方法。